Exploring Emotet, an elaborate everyday enigma

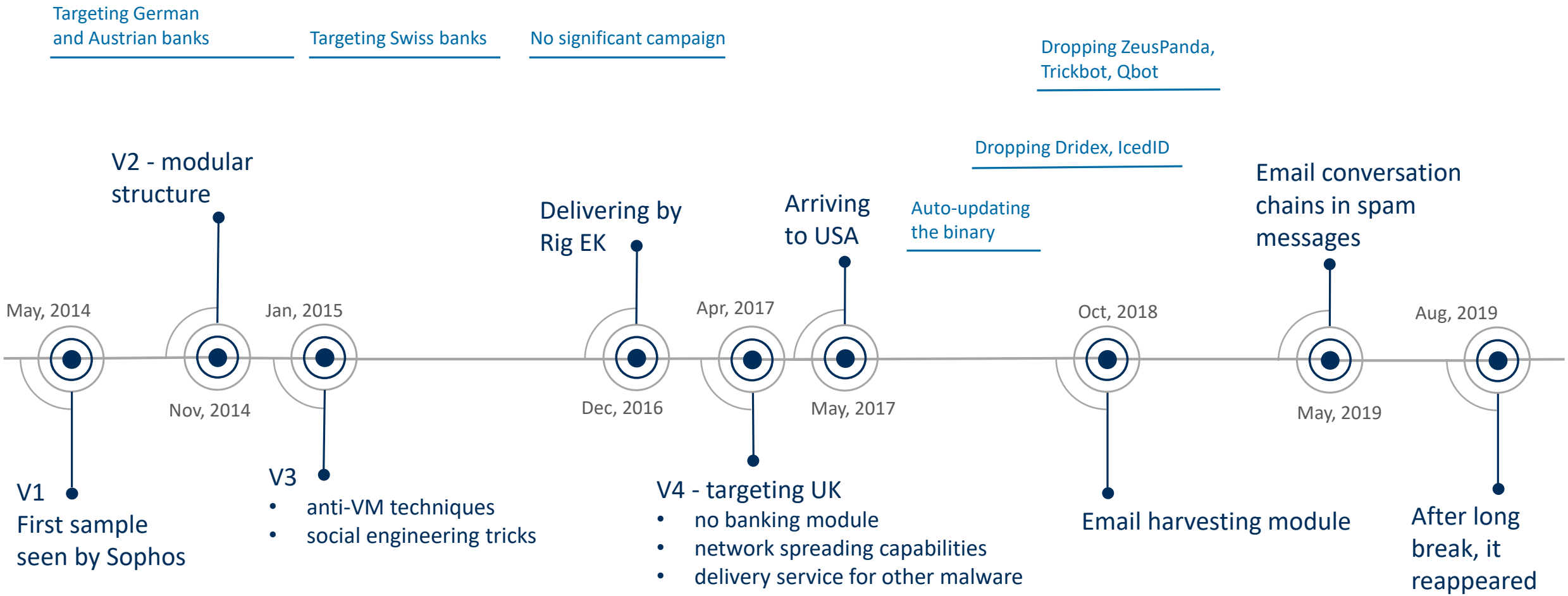
Luca Nagy

Threat Researcher, SophosLabs

Oct 2019

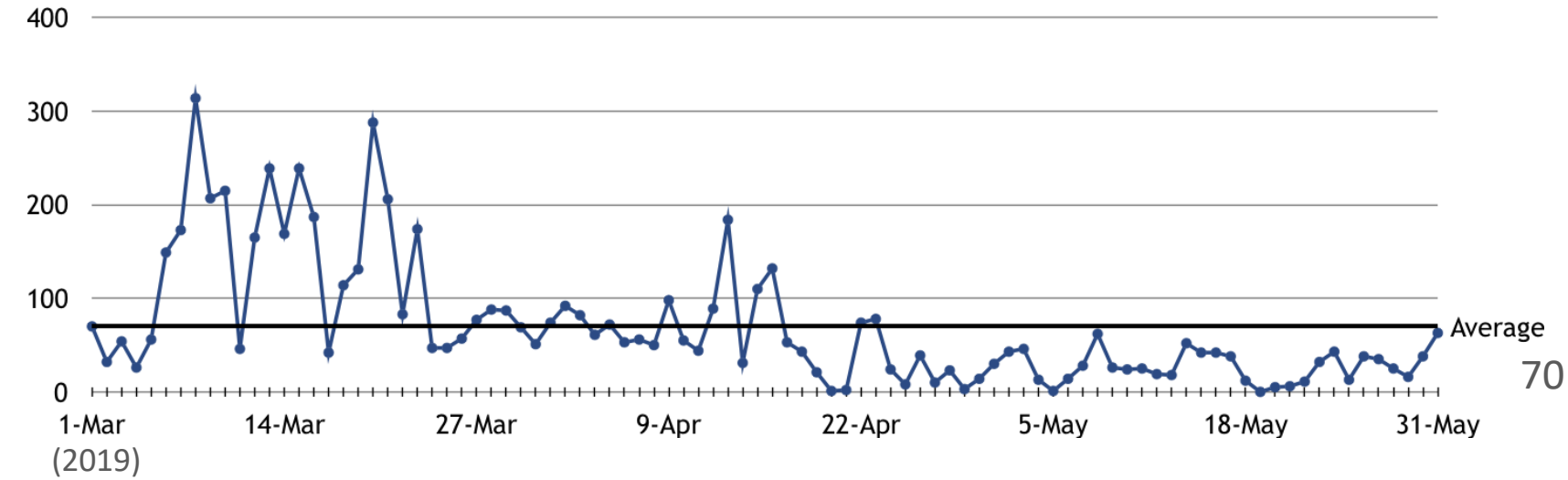
SOPHOS

History of Emotet



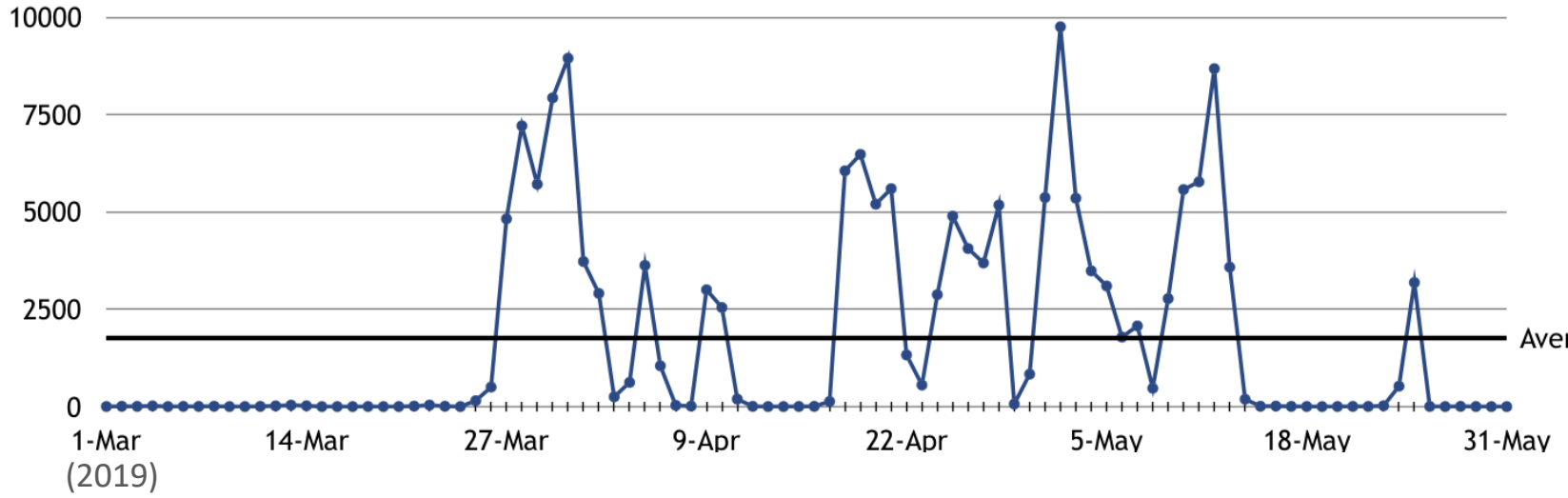
Unique binaries and downloaders on daily basis

New binaries



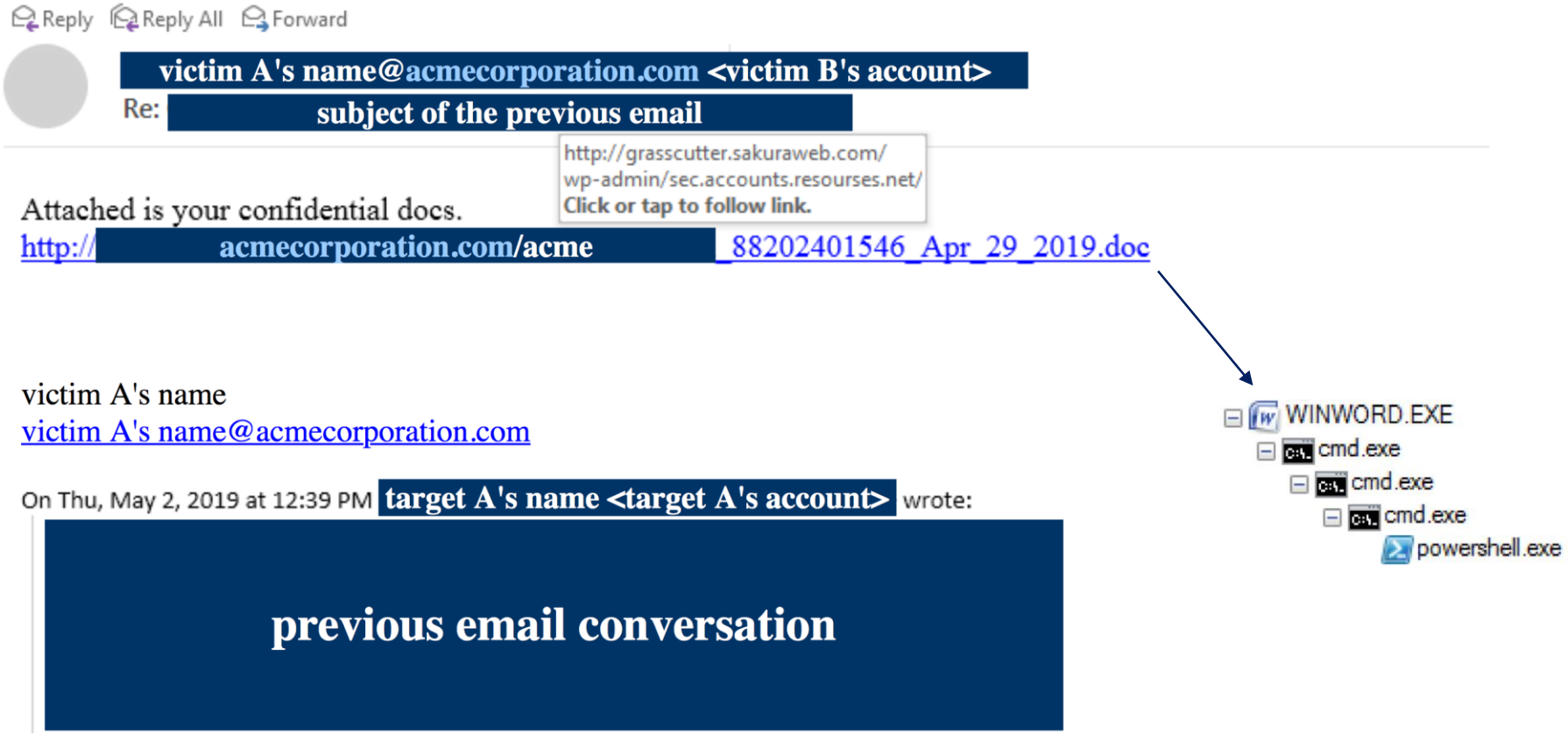
70

New downloaders



1763

Delivery method - Spam messages



Anti-analysis techniques: Anti-VM techniques, process injection

Anti-VM techniques

- Checking process list locally, using fake IP list
- Detecting VM, AV related files, folders
- Detecting sandbox environment
- Sending process list

Process injection

- Wrapper modules
- Heaven's Gate

Anti-analysis techniques: Injecting into 64 bit process - Heaven's Gate

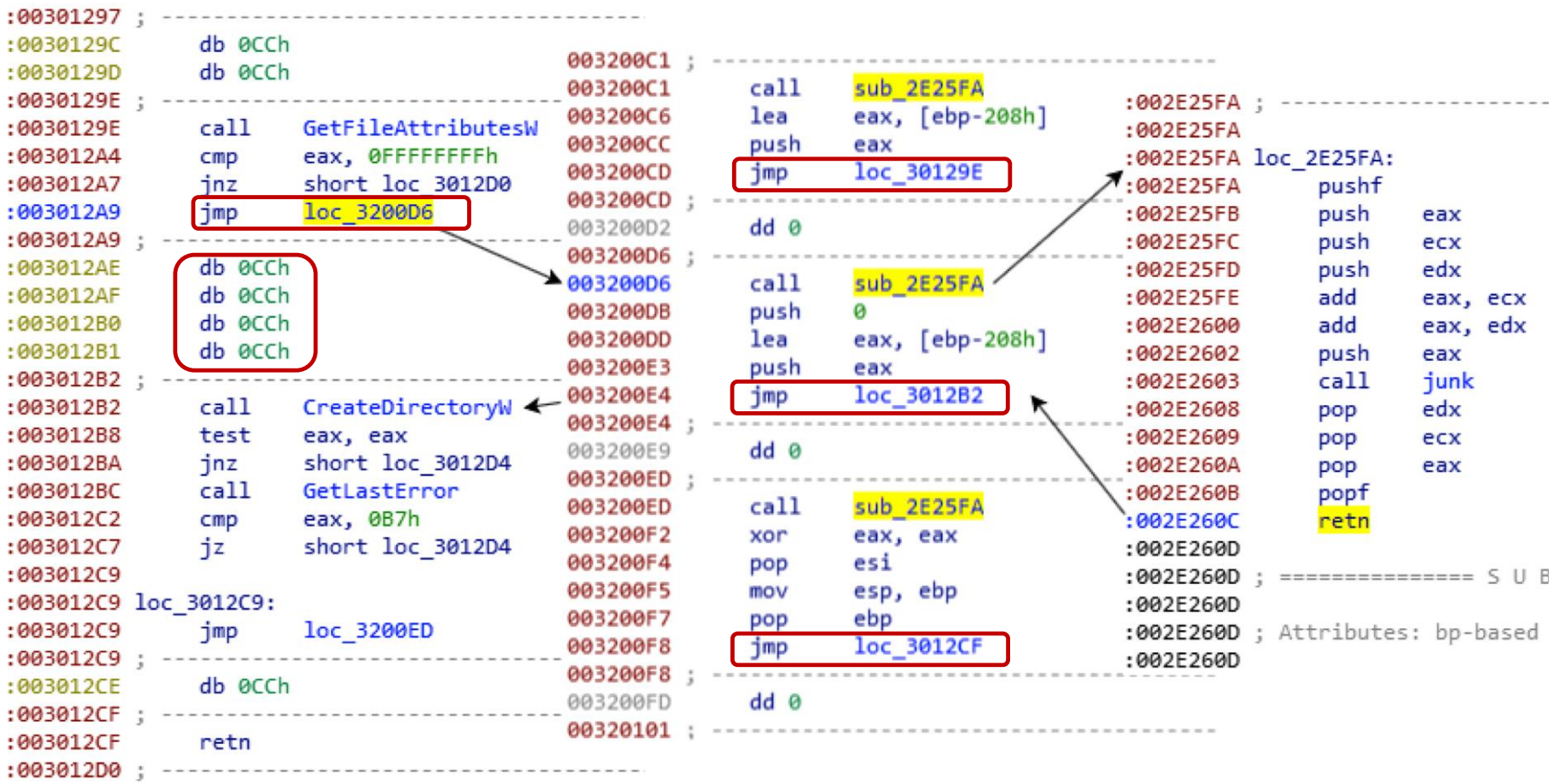
```
:02212A50
:02212A50                ; Attributes: bp-based frame
:02212A50
:02212A50                HeavensGate     proc far               ; CODE
:02212A50
:02212A50                var_8           = dword ptr -8
:02212A50
:02212A50 55                             push    ebp
:02212A51 8B EC                          mov     ebp, esp
:02212A53 6A 33                          push    33h
:02212A55 E8 00 00 00 00                 call    $+5
:02212A5A 83 04 24 05                    add     dword ptr [esp], 5
:02212A5E CB                             retf
:02212A5E                HeavensGate     endp ; sp-analysis failed
:02212A5E
:02212A5E                ; ---------------------------------------------------------------------------
:02212A5F B8                             db 0B8h
:02212A60 60                             db  60h ; `
:02212A61 00                             db    0
:02212A62 00                             db    0
:02212A63 00                             db    0
:02212A64 67                             db  67h ; g
:02212A65 65                             db  65h ; e
:02212A66 48                             db  48h ; H
:02212A67 8B                             db  8Bh
:02212A68 00                             db    0
:02212A69 48                             db  48h ; H
```

32 bit disassembler

```
0000000002212A50 55                      db  55h ; U
0000000002212A51 8B                      db  8Bh
0000000002212A52 EC                      db 0ECh
0000000002212A53 6A                      db  6Ah ; j
0000000002212A54 33                      db  33h ; 3
0000000002212A55 E8                      db 0E8h
0000000002212A56 00                      db    0
0000000002212A57 00                      db    0
0000000002212A58 00                      db    0
0000000002212A59 00                      db    0
0000000002212A5A 83                      db  83h
0000000002212A5B 04                      db    4
0000000002212A5C 24                      db  24h ; $
0000000002212A5D 05                      db    5
0000000002212A5E CB                      db 0CBh
0000000002212A5F                 ; ---------------------------------------------------------------------------
0000000002212A5F B8 60 00 00 00          mov     eax, 60h
0000000002212A64 67 65 48 8B 00          mov     rax, gs:[eax]
0000000002212A69 48 8B 40 18             mov     rax, [rax+18h]
0000000002212A6D 48 8B 40 30             mov     rax, [rax+30h]
0000000002212A71 8B 50 14                mov     edx, [rax+14h]
0000000002212A74 8B 40 10                mov     eax, [rax+10h]
0000000002212A77 E8 00 00 00 00          call    $+5
0000000002212A7C C7 44 24 04 23+         mov     dword ptr [rsp+4], 23h
0000000002212A84 83 04 24 0D             add     dword ptr [rsp], 0Dh
0000000002212A88 CB                      retf
0000000002212A88                 ; ---------------------------------------------------------------------------
```

64 bit disassembler

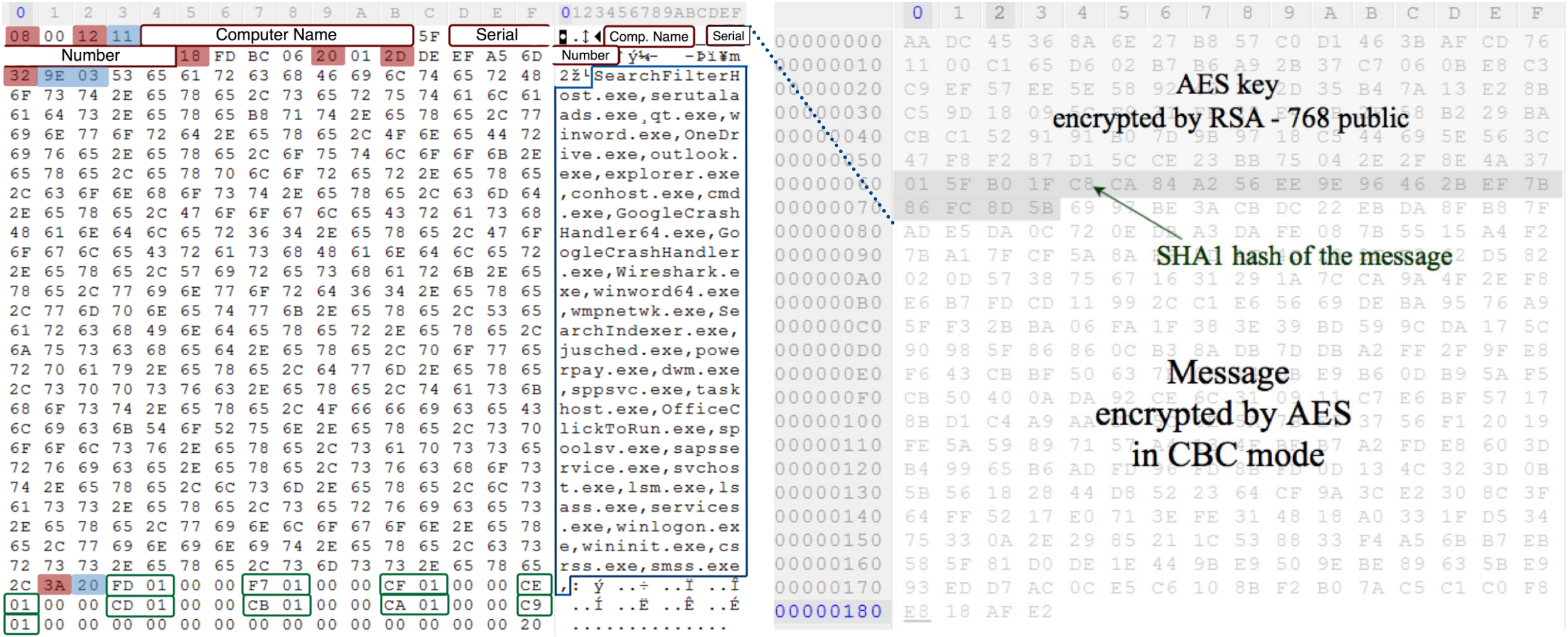
Anti-analysis techniques: Custom packer



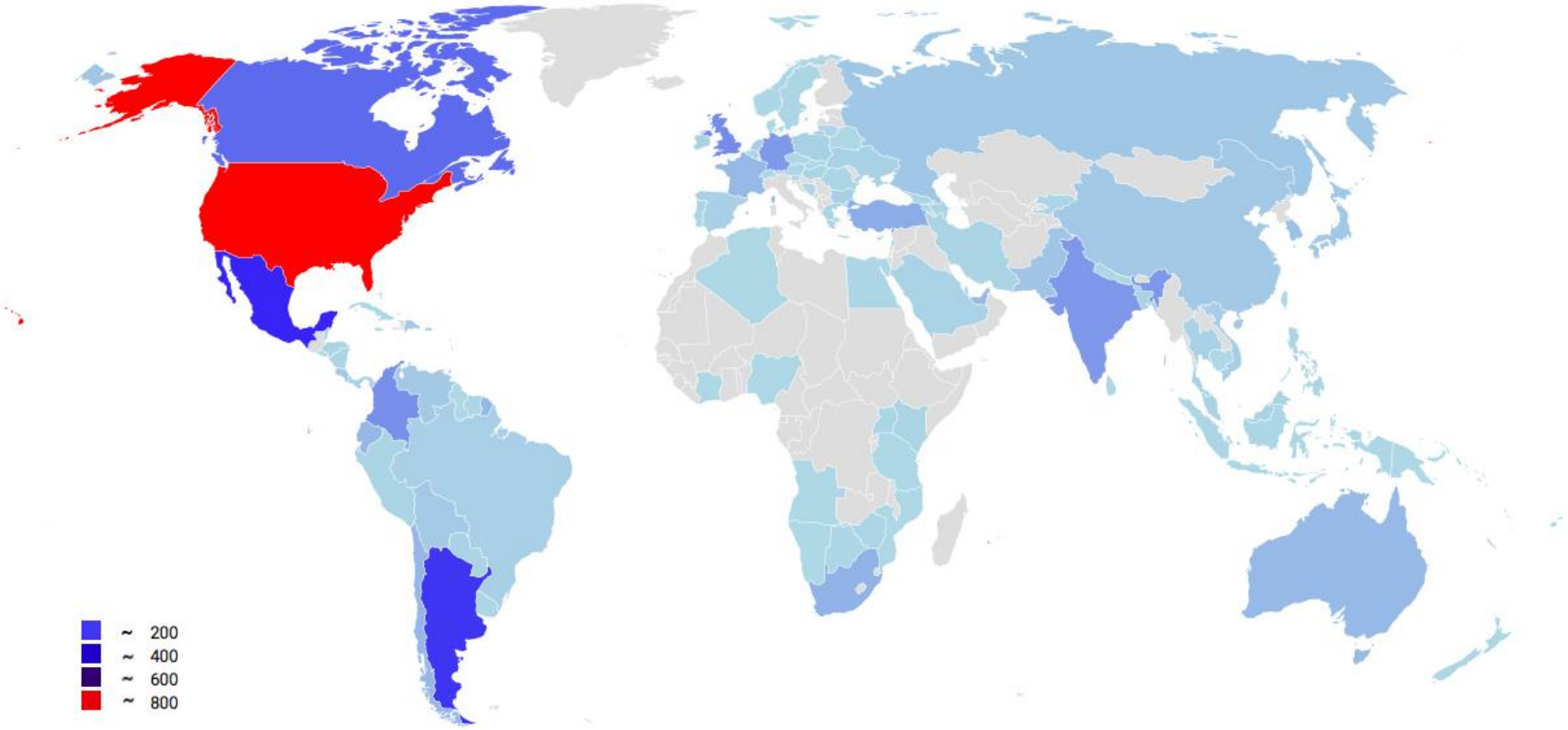
Main functions of the binary

```
    case 0:
      Advapi32(this);
      Shell32();
      if ( CreateProcessOrService() )           // %Appdata%
        goto exit;
      Value = 1;                                // CreateProcess -> false
      goto timeout_mod;
    case 1:
      Crypt32(this);
      Urlmon();
      Userenv();
      Wininet();
      Wtsapi32();
      if ( CryptoInit(v2) )                     // RSA - 768 and AES symmetric key
      {
        MachineNameVolumeInfo = machinename_volumeinfo;
        RSAencoded = &encoded_RSAkey;
        RSAencodedLenght = 106;
        Value = 2;
timeout_mod:
        result = GetTickCount() % 4000 + 4000;  // timeout to WaitForSingleObject
      }
      else
      {
exit:
        Value = 3;                              // case 3 -> ExitProcess
        result = 0;
      }
      return result;
    case 2:
      Value = 2;
      return C2Communication();
```

C2 server communication



IP address count used to reach the C2



Observed in the first 4 months of 2019

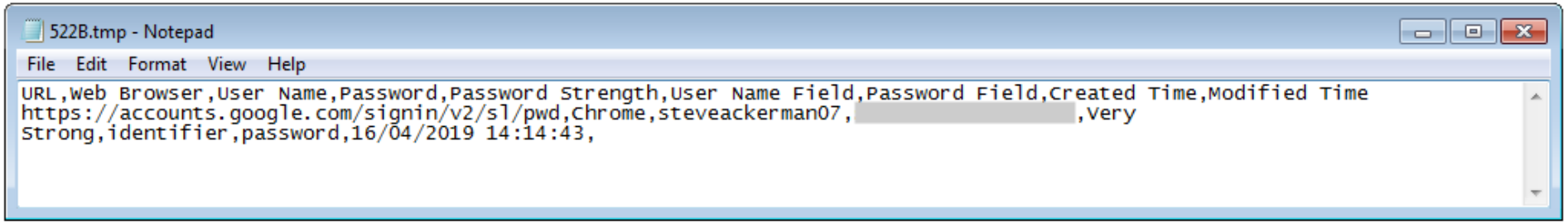
Downloaded Modules: Wrapper modules

```
MachineNameVolumeInfo = (int)this;
result = CreateEventW(0, 1, 0, 0);
event_handler = result;
if ( result )
{
  if ( Advapi32() && Crypt32() && Shell32() && Urlmon() && Userenv() && Wininet() && Wtsapi32() )
  {
    if ( GetTempPathW(260, &TmpFilePath) )
    {
      if ( GetTempFileNameW(&TmpFilePath, 0, 0, &TmpFilePath) )
      {
        DeleteFileW(&TmpFilePath);
        if ( CryptoInit(*(_DWORD *)(MachineNameVolumeInfo + 8)) )
        {
          if ( DecodeInject(v2) )
          {
            if ( ReadResult(&PTR_TMP_CONTENT) )
            {
              if ( !C2Communication(&PTR_TMP_CONTENT) )
              {
                do
                  time = GetTickCount();
                while ( WaitForSingleObject(event_handler, time % 4000 + 1000) == 0x102// 0x102 WAIT_TIMEOUT
                     && !C2Communication(&PTR_TMP_CONTENT) );
              }
```

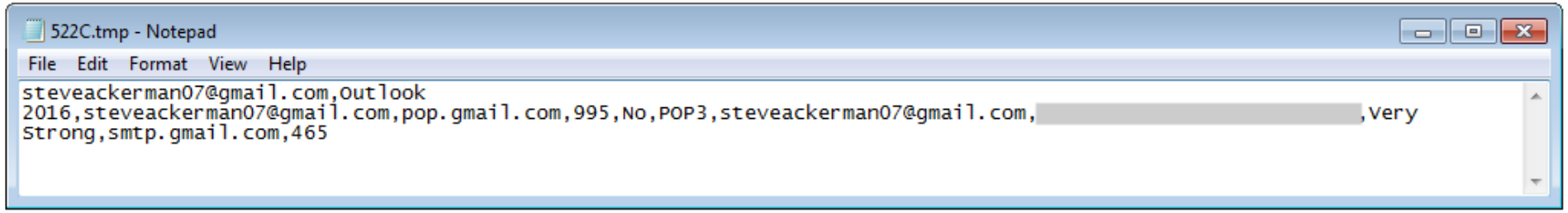
Inject into:

- /System32/alg.exe
- New instance of itself

Wrapper modules - Injected NirSoft executables

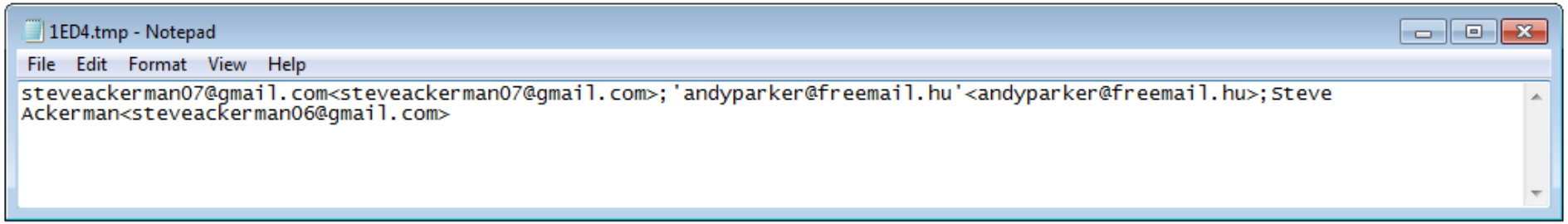


WebBrowser PassView

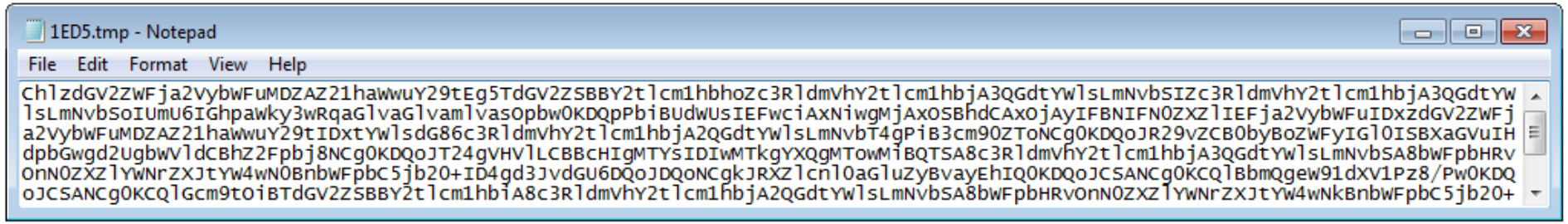


Mail PassView

Wrapper modules - Injected proprietary executables



Email contact extractor



Email content harvester

Regular modules: Network spreading module

- Enumerating SMB, null session connection

```
 94 13.160079   10.69.146.218   10.69.146.45    SMB2    154 Tree Connect Request Tree: \\ADAM1\IPC$
104 13.164308   10.69.146.218   10.69.146.45    SRVSVC  262 NetShareEnumAll request
108 13.166672   10.69.146.218   10.69.146.45    SMB2    158 Tree Connect Request Tree: \\ADAM1\ADMIN$
136 16.211525   10.69.146.218   10.69.146.45    SMB2    200 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \ADAM1\C$
138 16.212593   10.69.146.218   10.69.146.45    SMB2    150 Tree Connect Request Tree: \\ADAM1\C$
```

- Brute-forcing the connections (~10 000 passwords)

```
eyphed,eeeee1,evangeli,epson,eighty,hugohugo,hevnm4,howie,hoes,hooters1,honeydew,hounds,hellno,icecu
be,heretic,booper,bulls1,bulls23,buckaroo,bootleg,booyah,brent1,norfolk,nogard,nero,nexus6,neal,noun
ours,dave1,dante1,cyprus,derick,delpiero,corbin,collect,comets,cooper1,clueless,clticic,address,abbe
y1,aerosmit,tracy1,turtle1,tulane,valeria,tunnel,trousers,tusymo,totoro,prelude1,raphael,qhxbij,pvje
gu,prima,loves,mallorca,macgyver,makayla,lockout,ov3ajy,ozlq6qwm,drinks,doll,details,detect,dogggg,d
ivision,dunhill,sairam,rulz,rxmtkp,gforce,generals,garland,fubar1,fx3tuo,gldmeo,godboy,fwsadn,gaelic
,gocats,fortune12,fihdfv,fear,cardinals,ccccc1,chateau,candys,c7lrwu,chas,charlie2,5291,5858,5lyedn,
6bjvpe,7676,7kbe9d,greek,happydog,grammy,guns,gucci,hazmat,gooseman,auckland,bagpuss,barks,andyandy,
allman,archery,1019,1478963,1411,rasta220,roadway,renee1,robyn,reject,reboot,rockrock,reznor,riches,
```

Regular modules: UPNP module

- Port-forwarding

  Port numbers set by the module:

  20, 21, 22, 53, 80, 143, 443, 465, 990, 993, 995, 7080, 8080, 8090, 8443, 50000

  (Same as the port numbers used to reach the C2 – hardcoded in the binary)

- Bypassing firewall rules

- Verifying the settings

Regular modules: Spam bot module

- SMTP message sent by the spam bot module

```
220 email server Welcome to RaidenMAILD ESMTP service v3702, Tue, 19 Feb 2019 17:42:55 +0800, (C)2001-2017
EHLO victim C's IP
250-email server Hello email server IP
250-AUTH LOGIN
250-8BITMIME
250 SIZE 207257600
AUTH LOGIN
334 VXNlcm5hbWU6
victim B's username
334 UGFzc3dvcmQ6
victim B's password
235 Authentication successfully
MAIL FROM: victim B's account
250 victim B's account Sender OK
RCPT TO: target A
250 target A recipient verified
DATA
354 start mail input; end with <CRLF>.<CRLF>
Date: Tue, 19 Feb 2019 09:42:44 -0700
From: victim A's name <victim B's account>
To: target A
Message-Id: <U5VVVvVMOu69.QPLuJxq7szsox9xazISqpfIbez0YYmWdeGj7La@web.de>
Subject: Zweite Mahnung
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_Part_55710_2421818552.18193033572538617174"

------=_Part_55710_2421818552.18193033572538617174
Content-Type: multipart/alternative; boundary="----=_Part_29497_2076436829.42562231182823880675"
```

hijacked account = victim B

sender = victim A
receiver = target A

template

Delivered malware

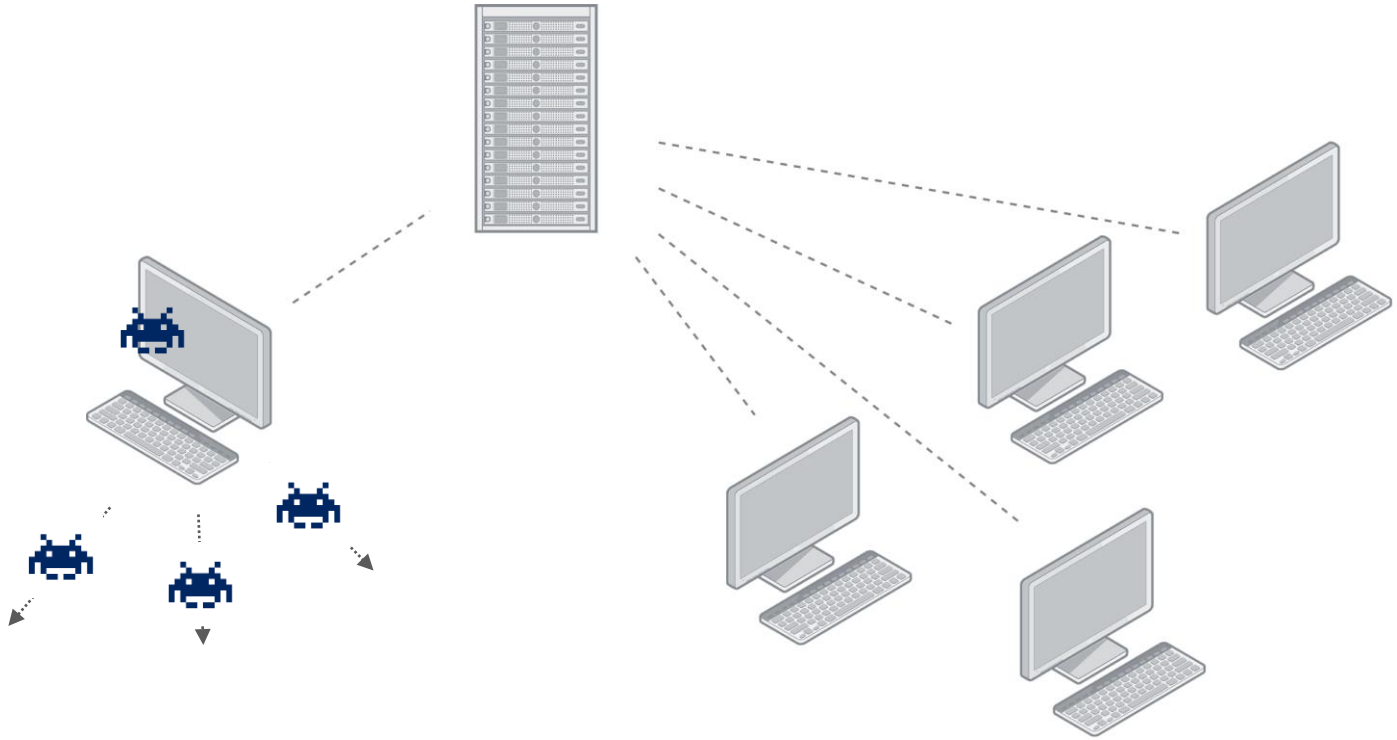
- Directly: Banking Trojans (e.g.: Trickbot, Qbot, Dridex, Ursnif, IcedID,…)
- Secondly: Ransomware (e.g.: Ryuk, BitPaymer, MegaCortex)
- Attack-chains:
  - Emotet – TrickBot – Ryuk
  - Emotet – Dridex – BitPaymer
  - Emotet – Qbot – MegaCortex

Sum up

- Information, credentials from browser

Sum up

- Information, credentials from browser
- Spreading through LAN

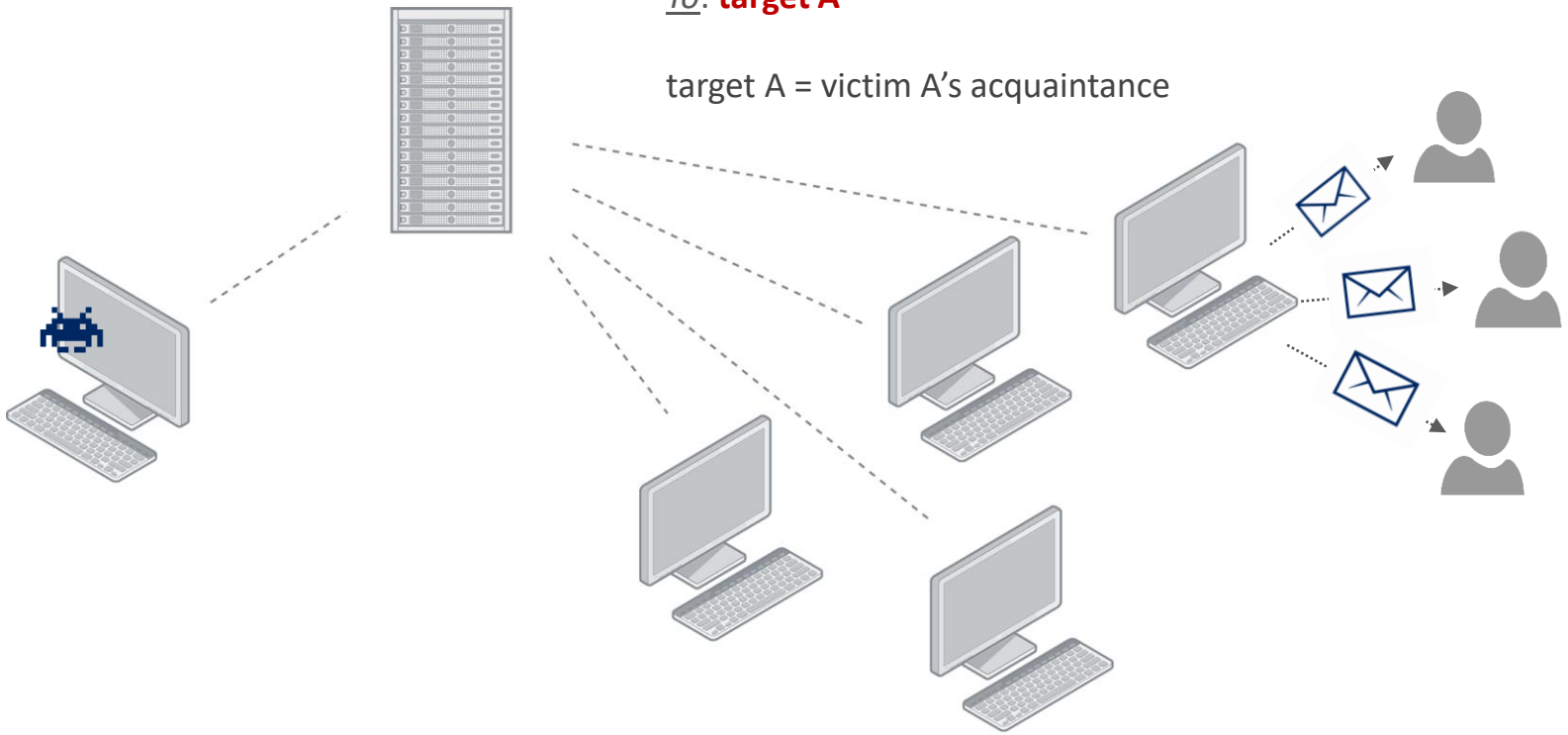


Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books

From: **victim A's name** <victim B's account>
To: **target A**

target A = victim A's acquaintance

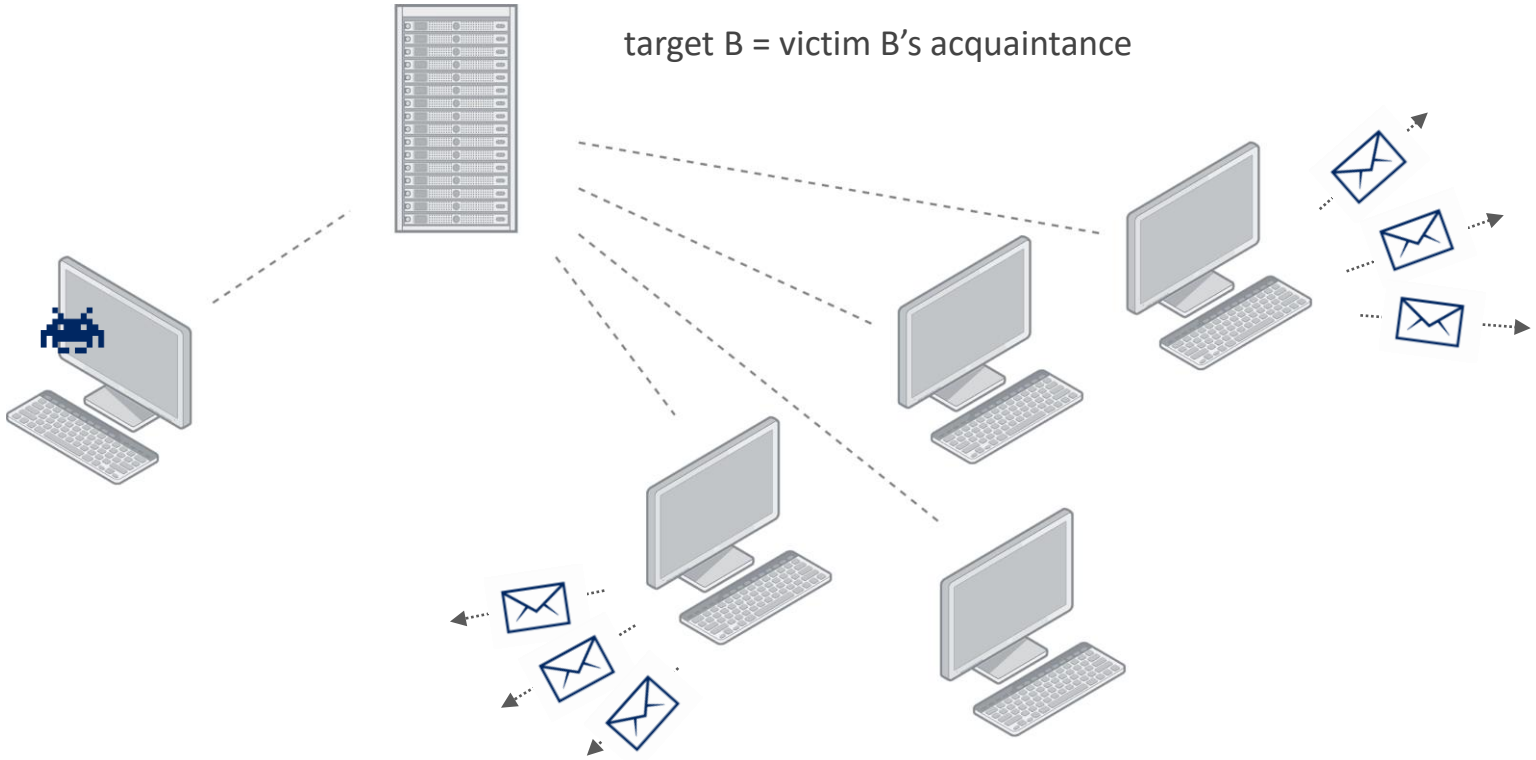


Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings

From: victim B's name <**victim A's account**>
To: target B

target B = victim B's acquaintance



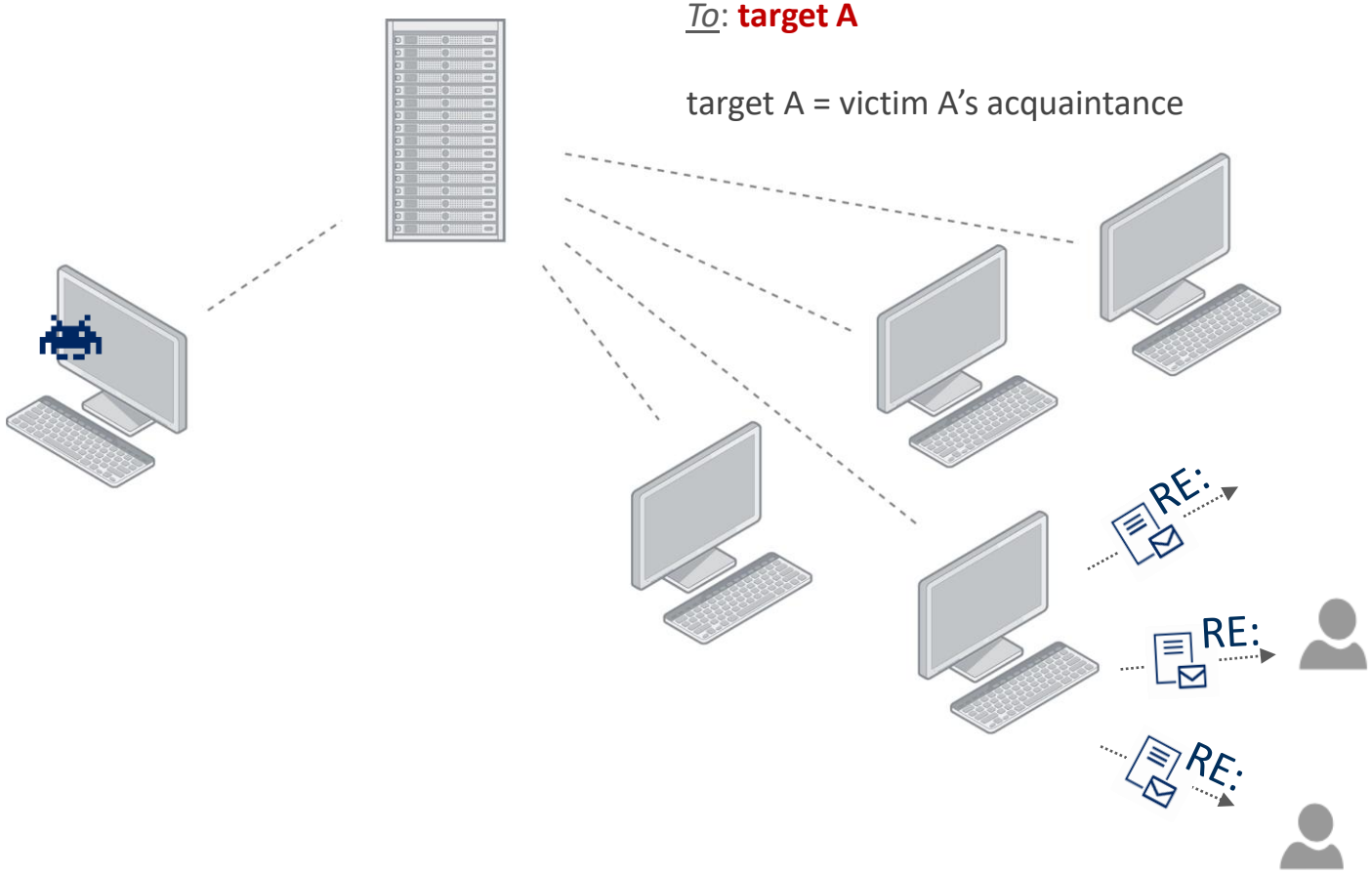
Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings
- Email conversation threads

Body: **victim A's email domain**/…/...zip

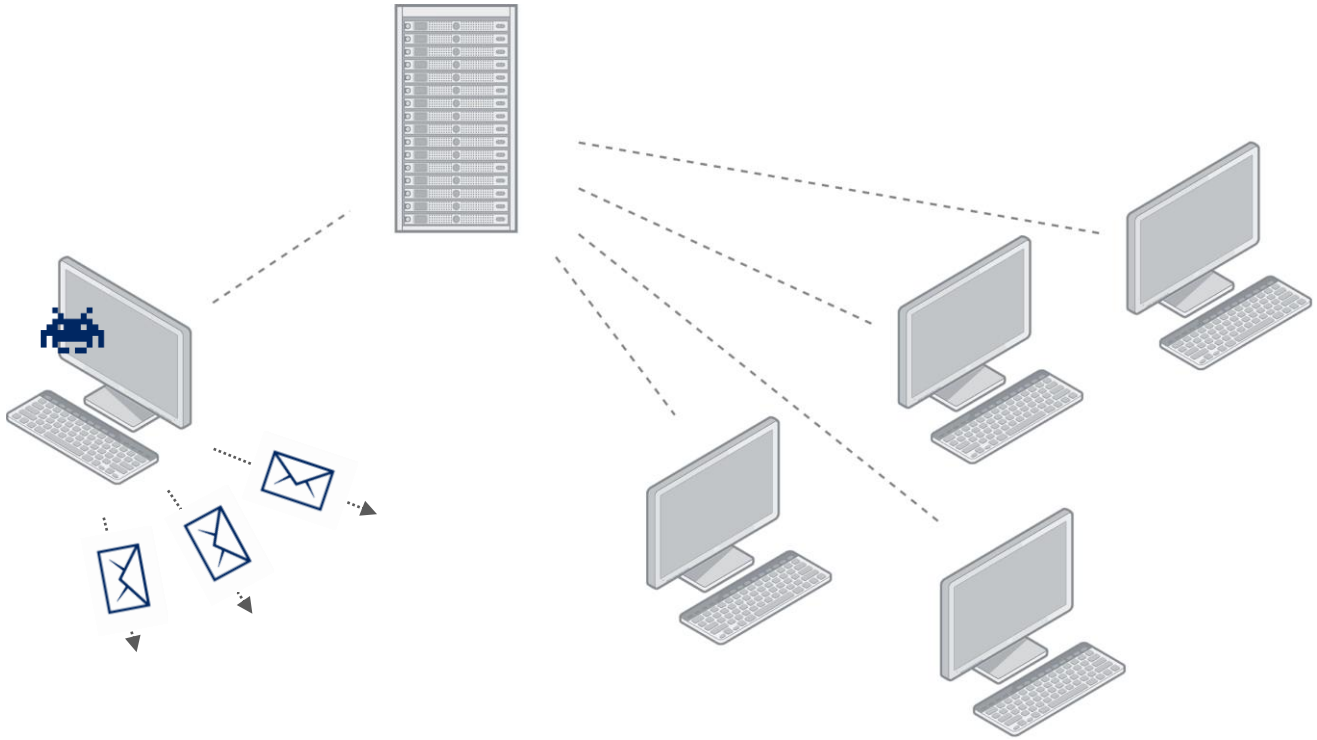
From: **victim A's name** <victim's B account>
Sub: **RE**:
To: **target A**

target A = victim A's acquaintance



Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings
- Email conversation threads
- Spamming



Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings
- Email conversation threads
- Spamming
- Proxy

Sum up

- Information, credentials from browser
- Spreading through LAN
- Email address books
- Email account settings
- Email conversation threads
- Spamming
- Proxy
- Deliver malware

?

Thank you!

Also thanks for:

- Gábor Szappanos
- Ferenc László Nagy
- Dorka Palotay
- SophosLabs

@luca_nagy_

SOPHOS